

ABSTRACT OF THE DISCLOSURE

A data copyright management system comprises a database for storing original data, a key control center for managing crypt keys, copyright management center for managing data copyrights, and a communication network for connecting these sections. Data supplied from the database to users is encrypted and distributed. The users decrypts the encrypted data by crypt keys obtained from the key control center or copyright management center. To supply data to users, there are the following two methods: a one-way supplying of encrypted data to users by means of broadcasting or the like; and two-way supplying of encrypted data to users corresponding to users' requests. A crypt key system used for encrypting data uses a secret-key cryptosystem, a public-key cryptosystem or a cryptosystem combining a secret-key and a public-key and further uses a copyright control program to control data copyrights. When a user stores, copies, or transfers data, the data is encrypted by a crypt key different from a crypt key used for supplying the data. The former crypt key is supplied from the key control center or from the copyright management center, or generated by the copyright control program. The present invention can be applied to a data copyright management system for using not only single data but also a plurality of data supplied from a single database or a plurality of data supplied from a plurality of databases. Further, an apparatus to be used by the user to perform data copyright management is proposed.